Date: **October 7, 2024**
To: **Scope and Program Committee**
From: **Addressing What Matters**
RE: **Proposal for Study Committee on Uniform or Model Act on Principal Office Definition**

I. Introduction

Addressing What Matters ("AWM") was formed for the purpose of "Protecting the social welfare, safety and privacy of small business owners, entrepreneurs, and independent contractors by promoting legislation that allows named individuals to retain residential privacy when submitting publicly viewable business filings to state authorities." While AWM is a fairly new organization, the need for residential privacy is well established. Myriad small business entities and entrepreneurs now operate their businesses absent a physical location. Thus, when submitting state business filings that mandate a principal office address, most of these business owners are forced to list their personal residential address to comport with state statutory requirements. However, our belief is that entities lacking a physical place of business should not be forced to provide a government authority with a residential address that will ultimately become part of a publicly available state record.

A significant minority of entities operate with no true physical location beyond the residences of their controllers. While this trend of decentralization has been gaining traction for years, the Covid-19 pandemic and associated "Stay-at-Home" orders catalyzed a transformation in digital infrastructure that turned remote business operations and employment from a niche offering to national mainstay. As the number of remote employers, employees, decentralized organizations, and short-term freelance workers continue to proliferate, the current definition of "Principal Office" grows increasingly out of touch with modern business trends and practices and is in need of revision.

To that end, AWM recommends that a study committee be appointed to consider the desirability of a uniform or model law, or revision of existing uniform or model law, regarding the definition of "Principal Office." A definition with more clarity and regard for the modern business landscape would complement existing laws as well as provide more certainty for entities lacking a physical business location. With many states adopting legislation recognizing decentralized entity forms as well as legislation to help various groups retain residential privacy, we expect that states would be extremely receptive to enacting a revised definition of "Principal Office" that properly balances the residential privacy concerns of individuals with the need to communicate with business entities.

II. Current Definitions of Principal Office

Among the fifty States, as well as the District of Columbia and Puerto Rico, statutory schemes defining "principal office" hinge upon the location of "the principal executive office of an entity."[1] Similar definitions are also found in both the Uniform Limited Liability Company Act[2] and the Model Business Corporation Act.[3] Essentially, what a state is asking for when requesting a principal office address is "where do the entity's decision makers make their decisions?" When business formation statutes that require a principal office address were first drafted, such a requirement was logical, as brick and mortar establishments were the unchallenged standard. Currently, approximately 2/3 of states have adopted a

1 *See generally* UNIF. LTD. LIAB. CO. ACT (UNIF. LAW COMM'N 2006) (most of the states that have defined "Principal Office" use this definition as the foundation.).

2 *Id.*

3 MODEL BUS. CORP. ACT (AM. BAR. ASS'N 2023).

statutory definition of principal office in line with the example provided above. Looking through the legislative histories of these states shows that, despite the underlying business code being adjusted occasionally, these definitions have rarely changed in any substantive way.

What these definitions fail to take into account is that technology has catalyzed a paradigm shift in how businesses operate and communicate. According to the Pew Research Center, "[w]hen looking at all employed adults ages 18 and older in the United States...about 14% – or roughly 22 million people – are currently working from home all the time."[4] As of 2023, 28.2% of this same group was working in a hybrid, or partially remote model.[5] Among all U.S. companies, approximately 67% offer some type of remote work with 16% having gone fully remote.[6]

These statistics show that the average, low-level employee is not the only one utilizing remote employment; companies' decision makers are also working away from the office, if an office exists at all. Thus, the answer to the question of "Where do the entity's decision makers make their decisions?" could be any number of personal residences for these remote entities.

Unrepresented in the statistics above are small, single member entities without employees. Limited liability company ("LLC") formations have multiplied in recent decades due to their ease of formation and management as well as the liability and asset protections they offer. While these entities may lack employees and fall outside of the remote employment statistics, the entrepreneurs who own and operate these entities are typically unburdened by the constraints of a physical office. Due to massive advances in technology over the last quarter-century, some entrepreneurs are able to run their business entities solely using a smartphone, creating a "digital-nomad" class of entrepreneurs with equally nomadic principal offices.[7]

As employees and entrepreneurs have become more decentralized, forming an entity anywhere in the nation has become extremely simple. With most states now offering online entity formation, creatives and resellers can easily form their own entity, or hire one of the dozens of online business formation services, and begin operations in mere hours. This convergence has led to a massive rise in the "gig" or freelance economy. Millions of Americans now supplement their primary income with their own small business earnings as an online seller or freelance worker, from the comfort of their home. These Residential Business Owners ("RBOs") have reconstructed how the U.S. economy functions.

Clearly, the landscape of modern business has changed; the statutory foundation that businesses are built upon must keep pace.

III. Residential Privacy Landscape: Federal Law

4 Kim Parker, *About a third of U.S. workers who can work from home now do so all the time*, PEW RESEARCH CENTER (Mar. 30, 2023), https://www.pewresearch.org/short-reads/2023/03/30/about-a-third-of-us-workers-who-can-work-from-home-do-so-all-the-time/.

5 Katherine Haan, *Remote Work Statistics And Trends In 2024*, FORBES (June 12, 2023, 5:29 AM), https://www.forbes.com/advisor/business/remote-work-statistics/.

6 *50 Eye-Opening Remote Work Statistics for 2024*, US CAREER INSTITUTE (Apr. 2024), https://www.uscareerinstitute.edu/blog/50-eye-opening-remote-work-statistics-for-2024#:~:text=16%25%20of%20U.S.%20companies%20are,to%20work%20remotely%20at%20all.

7 *See* Anita Campbell, *Can You Really Start a Business With Just a Smartphone? Yes!*, SMALL BUSINESS ADMINISTRATION (Sept. 22, 2016) https://www.sba.gov/blog/can-you-really-start-business-just-smartphone-yes. *See also* Sean Peek, *Can You Run a Business via a Smartphone?*, BUSINESS.COM (June 11, 2024), https://www.business.com/articles/run-business-from-smartphone/; *and* Brian Michelotti, *The Rise of Mobile Technology in Business: 5 Ways It's Shaping the Future*, ABERDEEN STRATEGY & RESEARCH (Mar. 30, 2023) https://www.aberdeen.com/blogposts/the-rise-of-mobile-technology-in-business-5-ways-its-shaping-the-future/.

The Corporate Transparency Act ("CTA"), perhaps the most impactful, business-centric federal legislation of this century, went into effect on January 1, 2024.[8] Under the CTA, beneficial ownership information for most entities registered to do business in the U.S. must be submitted to the Financial Crimes Enforcement Network ("FinCEN").[9] The goal of the CTA and its reporting requirements are to prevent and combat fraud, money laundering, terrorism and other financial crimes that undermine the U.S. financial system.[10] To that end, the business address of each entity as well as the residential address of each beneficial owner must be submitted to FinCEN.[11] Given the aims of the CTA and the fact that "transparency" is within its name, one might assume all of this information would be readily available to the general public. Thankfully, that is not the case. All information obtained by FinCEN is housed on private, encrypted databases and accessible only by law enforcement and other government officers.[12]

When promulgating the final rule related to beneficial ownership information reporting, FinCEN stated:

"In general, FinCEN recognizes the sensitivity inherent in collecting any personal identifying information and takes seriously the need to maintain the highest standards for information security protections for information reported to FinCEN to prevent the loss of confidentiality, integrity, and availability of information that may have a severe or catastrophic adverse effect."[13]

With the federal government acknowledging the need to keep residential address information private and confidential, modifying the definition of principal office to accommodate for such protections at the state level would be in line with current legislative trends.

<u>IV. Residential Privacy Landscape: State Law</u>

According to the U.S. General Services Administration, Personal Identifying Information ("PII") is defined, in part, as "sensitive information...that directly identifies an individual [including] name, personal/home address, social security number (SSN), financial banking information, other identifying number or code, home telephone number, personal email address, etc."[14] While PII has gained more attention in recent years due to an influx of enacted privacy and data protection laws, the principles behind the term were first established in the the Privacy Act of 1974.[15] Historically, one's personal address has been one of the least protected aspects of PII. When hard-copy phone books were commonplace, the personal addresses of most individuals that utilized landline telephones could be found within, unless you requested that the publisher omit your address. Thus, while most individuals were resigned to the idea of their personal addresses being accessible, the need to offer some privacy protections were known.

8 *See* 31 U.S.C. § 5336 (2021) *and* 31 C.F.R. § 1010.380 (2024).
9 31 C.F.R. § 1010.380(a).
10 Beneficial Ownership Information Reporting Requirements, 87 FED. REG. 59,498 (codified as 31 C.F.R. § 1010.380).
11 31 C.F.R. § 1010.380(a)-(b).
12 *Beneficial Ownership Information*, FIN. CRIMES ENFORCEMENT NETWORK (Jul. 24, 2024), https://www.fincen.gov/boi-faqs#:~:text=Beneficial%20ownership%20information%20reported%20to,at%20the%20highest%20security%20level.
13 Supra note 10, at 59,518.
14 *Rules and Policies - Protecting PII - Privacy Act*, U.S. GEN. SERV. ADMIN. (Aug. 11, 2023), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.
15 5 U.S.C. § 552a.

The proliferation of the internet and wireless and digital technology have made both landline telephones and phone books obsolete while exponentially increasing PII concerns. Whereas a phone book would be limited to localized personal address information, any unprotected address in the U.S. can now be found by anyone with an internet connection. Data breaches, identity theft, and the ability to purchase another individual's PII on the dark web have increased privacy concerns in recent years. The ease with which this information can be found put many vulnerable groups at risk and necessitated change.

In response, many states have enacted legislation to create Address Confidentiality Programs (ACP). To date, nearly 40 states have adopted some sort of ACP legislation.[16] The vast majority of these programs aim to protect victims of domestic violence, abuse and stalking by allowing victims to keep their addresses off of publicly accessible records. Sadly, highly public occurrences of threats of violence and actual violence against other groups have necessitated the expansion of ACP protections in many states.

Between 2021 and 2023, threats against federal judges and prosecutors rose sharply. In 2021, there were a reported 224 threats against federal judges, with that amount more than doubling, to 457, in 2023.[17] Threats against federal prosecutors also more than doubled within that time frame, jumping from 68 to 155.[18]

State Court Officers have also experienced a dramatic rise in reported threats. Between 2018 and 2023 within the State of Texas there were "522 general threats, 29 assaults, and 68 bomb threats...made toward judicial officers."[19] One of the most shocking instances came in 2015 when a gunman obtained the home address, phone number, and make and model of vehicle of Texas Judge Julie Kocurek, simply from online searches. The assailant stalked Judge Kocurek and her family for weeks before confronting and shooting her, causing serious injury.[20] This attack, along with the numerous other threats, prompted Texas to pass the address confidentiality legislation discussed below.

These types of threats are not confined to the judiciary. According to Forbes, "[m]ore than 40% of state lawmakers say they've experienced threats in the past three years, while nearly 20% of other local officeholders reported experiencing threats in the past year-and-a-half."[21] A staggering 90% of state lawmakers claimed to experience some form of "harassment, intimidation, and stalking."[22]

The occurrences detailed above have prompted many states to expand ACP protections to government employees, as well as other groups that may be targeted in politically motivated violence. In Idaho, law enforcement officers can request that their residential address be exempt from public disclosure.[23]

16 SAFE AT HOME, https://www.sos.mo.gov/business/SafeAtHome/AddressConfidentialityProgramsByState (last visited Aug. 23, 2024).

17 Joseph Tanfani, et al., *Exclusive: Threats to US federal judges double since 2021, driven by politics*, REUTERS (Feb. 13, 2024 at 8:55 AM), https://www.reuters.com/world/us/threats-us-federal-judges-double-since-2021-driven-by-politics-2024-02-13/.

18 *Id*.

19 *NCSC supports new legislation to protect state court judges from escalating threats*, NAT'L. CTR. FOR ST. CTS., https://www.ncsc.org/newsroom/at-the-center/2024/ncsc-supports-new-legislation-to-protect-state-court-judges-from-escalating-threats (last visited Aug. 23, 2024).

20 *Id*.

21 James Farrell, *Over 40% Of State Lawmakers Have Faced Threats—Leading Some To Avoid Polarizing Issues, Report Says*, FORBES, https://www.forbes.com/sites/jamesfarrell/2024/01/25/over-40-of-state-lawmakers-have-faced-threats-leading-some-to-avoid-polarizing-issues-report-says/ (Jan. 25, 2024 at 7:00 AM).

22 Vera Bergengruen, *Public Officials Face Surge of Threats Ahead of 2024 Election*, TIME, https://time.com/6565184/violent-threats-public-officials/ (Jan. 25, 2024 at 7:05 AM).

23 ID CODE § 19-5803 (2023).

Washington has extended ACP protections to criminal justice affiliates, elections officials, or protected health care workers who are a target for threats or harassment.[24] Texas allows judges, U.S. Marshals, certain government attorneys and peace officers to apply to their "Alternate Address Program" in order to keep their residential addresses private in certain contexts.[25] New York's ACP protections can apply to reproductive health care services providers and their employees, volunteers, and patients, as well as the immediate family members of reproductive health care services providers.[26]

ACP protections for RBOs were not mentioned above, and, to date, no state has enacted such protections. The inability to accurately track threats against RBOs is one possible reason ACP protections are currently unavailable. Threats against government officials typically draw headlines and broader investigations; further, the pool of those impacted is smaller and more closely knit, due to being part of a larger governmental body which can track all reported threats. When RBOs are threatened or harassed, their sole recourse is to file a police report or resort to social media. While RBOs may be part of a local chamber of commerce or other business community, there is no broader body to which threatened or harassed RBOs can report their concerns.

The lack of ACP protections coupled with the current definition of principal office put RBOs in a precarious position; the complete inability to protect their residential address, again a key component of PII, leaves RBOs vulnerable to all manner of threats. In recent years, two new forms of harassment have been implemented by bad actors: doxxing ("the gathering and publication of personal information such as addresses and phone numbers by hostile parties to try to intimidate and direct violence at someone") and swatting ("a fake report [to law enforcement] of a hostage situation, bomb, or other critical incident at the target's address, resulting in an overly militarized team being sent to confront the target or their family").[27] The ACLU has published guidance in how to deal with and avoid such threats, with minimizing public access to one's residential address being a primary step[28]; a step RBOs are currently unable to take.

The question, then, is not what dangers do RBOs face, but rather what are the best means of preventing the danger. Although ACP protections were discussed above, making RBOs a protected class in each state would be a major undertaking, especially in those states that do not have ACP legislation. Rather, the most efficient means of protecting RBOs PII is to revise the definition of principle office to be more inline with modern business trends and respect residential privacy.

V. Proposed Revision to Principal Office Definition

As detailed in the Sections above, the definition of Principal Office is in need of revision to better fit current, established business needs and methods. However, the need for residential address protections, obviously, does not apply to all entities. Many of the registered entities within the U.S. are still standard brick and mortar businesses capable of listing a physical address in line with current Principal Office definitions. As such, any revised definition of Principal Office must account for both options.

---

24 *See* RCW 9A.46.020 *and* 9A.90.120.

25 *Address Confidentiality*, TEXAS SECRETARY OF STATE (Nov. 2023), https://www.sos.state.tx.us/elections/laws/address-confidentiality.shtml.

26 *Address Confidentiality Program (ACP)*, NEW YORK STATE DEPARTMENT OF STATE, https://dos.ny.gov/ACP.

27 Jay Stanley & Daniel Kahn Gillmor, *Some Steps to Defend Against Online Doxxing and Harassment*, ACLU, https://www.aclu.org/news/free-speech/some-steps-to-defend-against-online-doxxing-and-harassment (Nov. 30, 2023).

28 *Id*.

With the above in mind, AWM proposes the following revised definition of Principal Office for consideration by a study committee:

I. "Principal Office" means:
   A. The location, within or outside of the state where:
      1. The Principal Executive of the entity maintains an office; or
      2. Major decisions impacting the entity are made; or
      3. Any physical street address under the control of the entity and so designated by the entity.
   B. If the entity does not have a "Principal Office" as described in subsection (A) of this section, then the address of the registered agent appointed by the entity in this state may be used, if authorized by the registered agent.

The proposed definition above both expands upon the current definitions of Principal Office while also including a small exception that can be utilized by RBOs. By elaborating on the standard "where the principal executive office of the entity is located," the ambiguity found in most current definitions is reduced, if not eliminated. Further, the exception established in subsection (B) is minor enough not to disrupt other elements of business entity codes and can be overseen by the appointed registered agent. Finally, as revised, additional investigative oversight by under state business services divisions would not be necessary.

<u>VI. Role of Registered Agents</u>

As detailed in the proposed language above, modifying the definition of Principal Office to allow RBOs to list the address of their registered agent as their principal office address would directly solve the PII concerns explained in Section IV. Implementing this change would also require little effort on the part of states. Almost all states allow an entity registered to do business within the state to serve as another entity's registered agent. Many states have additional requirements for entities specializing in registered agent services, or Commercial Registered Agents ("CRA").[29]

The appointment of a registered agent ensures that the state and interested parties have a valid point of contact for notices and service of process for each entity doing business within the state. This appointment alone makes the requirement of a principal office redundant. In states that do place additional reporting requirements on a CRA, the need is further reduced as a CRA must maintain accurate contact information with the state at all times or risk fines or business forfeiture.

From a global perspective, the practice is commonplace. The registered office of an entity in most foreign jurisdictions is often the address listed on governmental filings as opposed to the entity's principal office address, though the registered agent industry in foreign jurisdictions is often more highly regulated due to the overlap with trustee, banking, and nominee services. States could, however, find a happy medium by allowing entities to list the address of their registered agent as their principal office address but require that registered agents in the state maintain an individual communication contact with each client entity which includes a verified address.

<u>VII. Preventing Fraud</u>

---

29 *See e.g.*, WY STAT. § 17-28-105 (2022)

Many states are currently experiencing a massive influx of fraudulent business filings. These filings range from the simple, such as being signed and submitted by an unauthorized person, to the complex, such as reinstating an inactive entity and stealing the PII of the previous owners to defraud customers. With fraudulent filings becoming pervasive in some states, it is no wonder that omitting identifying information from a business filing would be a point of contention.

Those who favor the current definition of principal office would likely argue that there is an unequivocal need to know where a business is physically located should the business need to be contacted by the state or become embroiled in litigation and need to be served process; however, that rationale falls apart under even light scrutiny. As stated above, the statutory role of a registered agent is to be the communication proxy between the state or interested parties needing to serve process on the entity. Thus, the requirement that an entity appoint a registered agent alleviates the need to know where the entity is physically located. Further, if states cannot verify the accuracy of provided information, of what use is it?

Understanding the role that state governments play in the business formation process is key to understanding why requiring a principal office address under the traditional definition is increasingly inconsequential. State examiners who process business filings are predominantly constrained to "Ministerial Acts," which is generally defined as "an act performed in a prescribed manner and in obedience to a legal authority, without regard to one's own judgment or discretion."[30] More succinctly, state examiners must approve business filings if they conform to statute. Though the need for Ministerial Acts is readily apparent, the absence of examiner discretion creates easily exploitable holes in which bad actors may thrive by providing fraudulent information that appears to conform to statutory requirements. However, by leveraging preexisting relationships with registered agents, as described above, business services divisions can actively combat fraud despite the trappings of a ministerial role.

One of the core components in fostering a business friendly environment is a clear, concise and, most importantly, expedient business formation and filing process. To that end, states have generally made the review of business filings a ministerial act so applicants know that, if they submit what is required, there should be no administrative roadblocks to forming and maintaining their business. If formation and filing statutes did not prescribe ministerial duties to examiners, they would be subject to examiner discretion and individual fiat. Obviously, no individual should be the gatekeeper of a state's business formation and filing process. Applicants need to know exactly what is required, and ministerial acts achieve that purpose and promote efficiency.

However, legislation is about balance. While making examiner review of formations a ministerial act does help eliminate the potential bias noted above, the robotic nature of a ministerial act presents its own set of issues. Consider this scenario: An examiner is reviewing a business formation filing. All of the necessary fields are complete, but the addresses listed for the entity and its registered agent are a vacant lot and gas station, respectively. While these facts point towards fraud, under most state business formation statutes the examiner would be forced to approve the filing because the provided addresses are presumably valid and the examiner lacks discretion and investigative authority. With many filings now completed instantaneously online, individual discretion is removed even beyond the ministerial act.

30 *Ministerial Act*, WEX LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex (last visited Aug. 26, 2024).

Another consideration that must be weighed is that of state resources. Any level of investigation associated with a business filing would incur costs. Any level of post-investigative enforcement would incur additional costs and possibly raise due process considerations. The digitalization of business has decreased the importance of physical location and put states in competition with each other to attract new businesses. If State A slows their business formation process to allow for the full investigation of provided information, entities will flock to State B that allows instantaneous online flings.

While fraudulent business filings are a major concern across the country, the vast majority of business filings are legitimate. Thus, states have rightfully chosen to prioritize efficiency rather than committing their finite resources to investigation and enforcement. So the question then becomes, what can be done to stymie fraudulent filings without sacrificing filing efficiency? How can states not only foster business creation but also prevent fraudulent entities from propagating? Again, with registered agents providing a reliable address to the state and doing their own due diligence to obtain client contact information, the concern of fraud can be minimized and, possibly, abated.

VIII. Conclusion

Appointing a study committee to consider the desirability of a uniform or model law, or revision of existing uniform or model law, regarding the definition of "Principal Office" would modernize business codes and help to protect the residential privacy of modern entrepreneurs. Further, state law would move more in line with recent federal legislation helping to create national uniformity. By minimizing the reach and scope of the change, states could easily adopt and implement the new definition. By utilizing preexisting relationships with the registered agent community, states can better combat fraudulent filings.

IX. Stakeholders

- Northwest Registered Agent LLC